Jurnal TICOM: Technology of Information and Communication
Volume 13, Nomor 2, Januari 2025 Hal: 92-97 E-ISSN: 2962-7982

Pembuatan GH3RTZ *Framework* untuk Proses *Reconnaissance* dan Deteksi Celah Keamanan

Muhamad Givari Ramadan[1*], Mardi Hardjianto[2]

[1,2] Fakultas Teknologi Informasi, Teknik Informatika, Universitas Budi Luhur, Jakarta, Indonesia
Jl. Raya Ciledug, Petukangan Utara, Pesanggrahan, Jakarta Selatan 12260
Email: [1*]2011501000@student.budiluhur.ac.id, [2]mardi.hardjianto@budiluhur.ac.id
(*: corresponding author)

Abstrak*— Penelitian ini mengkaji kemampuan GH3RTZ *framework* dalam mendeteksi kerentanan keamanan pada tahap *reconnaissance*, yang merupakan langkah awal penting dalam pengujian penetrasi. Di era digital, dominasi teknologi informasi membawa manfaat besar namun juga tantangan signifikan terkait keamanan data, yang dapat mengancam informasi sensitif organisasi jika tidak dikelola dengan baik. Untuk mengatasi tantangan ini, penelitian ini menggunakan metode *grey box testing* dan Algoritma *Boyer-Moore*, yang dipilih karena kemampuannya dalam mencocokkan *string payload* dengan sistem website untuk mengidentifikasi kerentanan pada tahap *reconnaissance*. Tahapan penelitian mencakup pengujian fungsi utama dari GH3RTZ *framework*, termasuk *subdomain finder*, *parameter finder*, *XSS injection*, dan *open redirect scanner*. Hasil pengujian menunjukkan bahwa GH3RTZ *framework* berhasil mengidentifikasi *subdomain* dan *parameter*, mendeteksi kerentanan *XSS* dengan *payload* tertentu, dan mengenali kerentanan *redirect* dengan *payload* spesifik. Kontribusi utama dari penelitian ini adalah pengembangan dan implementasi GH3RTZ *framework*, yang tidak hanya mampu mendeteksi kerentanan pada tahap *reconnaissance*, tetapi juga mudah diimplementasikan oleh individu dan organisasi kecil hingga menengah, sehingga meningkatkan kesadaran dan keamanan siber secara keseluruhan. Hasil pengujian menunjukkan bahwa *framework* ini secara signifikan meningkatkan deteksi kerentanan.

Kata Kunci— **Keamanan Siber, Pengujian Penetrasi, *Grey Box Testing*, Algoritma *Boyer-Moore*, GH3RTZ *Framework*, Kerentanan Keamanan.**

Abstract— ***This study examines the GH3RTZ framework's ability to detect security vulnerabilities during the reconnaissance phase, a critical initial step in penetration testing. In the digital era, the dominance of information technology brings both significant benefits and challenges, particularly regarding data security, which can threaten an organization's sensitive information if not properly managed. To address these challenges, this study employs grey box testing and the Boyer-Moore Algorithm, chosen for its capability to match payload strings with website systems to identify vulnerabilities during the reconnaissance phase. The research process involved testing the core functions of the GH3RTZ framework, including the subdomain finder, parameter finder, XSS injection, and open redirect scanner. The results showed that the GH3RTZ framework successfully identified subdomains and parameters, detected XSS vulnerabilities with specific payloads, and recognized redirect vulnerabilities with specific payloads. The primary contribution of this research is the development and implementation of the GH3RTZ framework, which not only effectively detects vulnerabilities during the reconnaissance phase but is also accessible for implementation by individuals and small to medium-sized organizations, thereby enhancing overall cybersecurity awareness. The testing results indicate that this framework significantly improves the detection of vulnerabilities.***

Keywords— **Keamanan Siber, Pengujian Penetrasi, *Grey Box Testing*, Algoritma *Boyer-Moore*, GH3RTZ *Framework*, Kerentanan Keamanan**.

I. PENDAHULUAN

Di era digital yang terus berkembang, teknologi informasi memainkan peran penting dalam berbagai aspek kehidupan, mulai dari komunikasi hingga pelayanan kesehatan. Meskipun kemajuan ini memberikan banyak manfaat, tantangan baru terkait keamanan dan privasi data juga muncul. Menjaga keamanan informasi dan sistem komputer menjadi sangat penting untuk melindungi privasi dan keamanan pengguna [1]. Baik organisasi besar maupun kecil semakin menyadari pentingnya melindungi data sensitif mereka dari serangan siber yang dapat merusak reputasi dan keberlanjutan bisnis mereka [2].

Dalam lingkungan informasi yang kompleks saat ini, layanan informasi dan teknologi perusahaan sangat rentan terhadap risiko keamanan, termasuk kebocoran data sensitif dan gangguan akses yang berkepanjangan. Ancaman ini tidak hanya dapat menyebabkan kerugian finansial, tetapi juga berdampak signifikan pada operasional sehari-hari dan reputasi perusahaan.

Keamanan siber menjadi fokus utama dalam upaya melindungi sistem komputer dan data dari ancaman seperti pencurian atau gangguan. Salah satu metode yang efektif untuk mengidentifikasi dan mengatasi potensi celah keamanan adalah pengujian penetrasi, yang melibatkan simulasi serangan terhadap sistem untuk menemukan dan memperbaiki kelemahan sebelum dieksploitasi oleh pihak yang tidak bertanggung jawab.

Dalam konteks pengujian penetrasi, tahap *reconnaissance* atau pengintaian adalah langkah penting. Pengumpulan informasi awal yang komprehensif, seperti identifikasi *subdomain* dari *domain* utama, menjadi krusial untuk mengeksplorasi potensi kerentanan yang ada.

Framework berbasis *web* seperti GH3RTZ *framework* hadir sebagai solusi yang mengotomatisasi proses pengumpulan data dan analisis. Dibandingkan dengan metode *manual* yang memakan waktu dan sumber daya besar,

penggunaan *framework* ini tidak hanya meningkatkan efisiensi tetapi juga akurasi dalam mengidentifikasi kerentanan. Hal ini sangat penting, terutama bagi organisasi dengan keterbatasan sumber daya yang tetap ingin memastikan tingkat keamanan yang tinggi.

GH3RTZ *framework* menjadi sangat relevan dalam menghadapi tantangan dengan teknik serangan yang semakin canggih dan kompleks. Solusi otomatis seperti *framework* ini mendukung pencegahan serta deteksi dini terhadap potensi ancaman keamanan. Diharapkan, penggunaan GH3RTZ *framework* tidak hanya dapat meningkatkan keamanan sistem informasi secara keseluruhan tetapi juga membantu organisasi kecil dan menengah dalam menghadapi tantangan keamanan siber yang terus berkembang, serta menjaga integritas data mereka yang semakin penting.

Penelitian ini berfokus pada evaluasi efektivitas GH3RTZ *framework* dalam tahap *reconnaissance* dari pengujian penetrasi, untuk mendeteksi potensi kerentanan dan mengumpulkan informasi yang diperlukan dalam menilai keamanan situs web. Hasil penelitian ini diharapkan dapat memberikan wawasan tentang bagaimana *framework* ini dapat membantu individu dan organisasi kecil hingga menengah dalam meningkatkan keamanan situs web mereka sebelum celah tersebut dieksploitasi oleh pihak yang tidak bertanggung jawab.

II. METODE PENELITIAN

A. Proses Pengujian Keamanan Siber

1) Tahap *Reconnaissance* dalam *Penetration Testing*

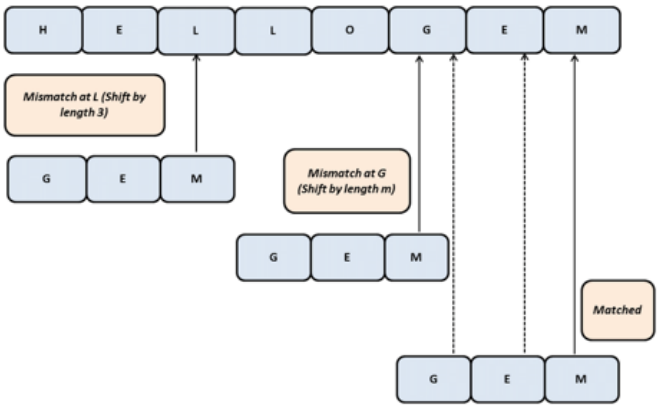
Tahap *reconnaissance* adalah tahap awal yang bertujuan untuk memahami target serangan secara menyeluruh. Metode umum dalam tahap ini meliputi *Google dorking*, *scraping website*, dan lainnya. Kelemahan dari metode *manual* adalah keterbatasan waktu dan efisiensi, yang dapat diatasi dengan *automation testing*. *Automation testing* meningkatkan efisiensi dan konsistensi serta dapat mengurangi beban kerja penguji.

2) Peran *Framework* dalam Mendukung *Penetration Testing*

Framework penetration testing memainkan peran krusial dengan menyediakan struktur dan alat yang diperlukan untuk otomatisasi dan pengumpulan informasi. Dengan integrasi berbagai alat seperti pemindai kerentanan, *framework* ini tidak hanya meningkatkan efisiensi tetapi juga efektivitas proses pengujian, serta mempermudah pelaporan dan dokumentasi hasil [3].

3) Algoritma *Boyer-Moore* dalam Pencocokan *String*

Algoritma *Boyer-Moore* adalah salah satu metode efisien untuk pencocokan string yang menggunakan pendekatan heuristik. Algoritma ini bekerja dengan mencocokkan pola dari kanan ke kiri dan menggunakan tabel heuristik untuk mempercepat proses pencocokan, sehingga mengurangi jumlah perbandingan yang diperlukan dan meningkatkan kecepatan pencarian [4].



Gambar 1. *Algoritma Boyer-Moore*

4) Algoritma *Boyer-Moore* dan Pencocokan *XSS* serta *Open Redirect Payload*

Algoritma *Boyer-Moore* sangat berguna dalam mendeteksi *payload* berbahaya untuk *Cross Site Scripting (XSS)* dan *Open Redirect*. Efisiensinya dalam pencocokan pola memungkinkan deteksi cepat dan akurat dari pola-pola berbahaya yang ada dalam daftar payload yang telah diketahui.

5) Metode dan Teknik Pencarian *Cross Site Scripting (XSS) Payload*

Dalam pencarian *XSS Payload*, terdapat dua metode utama: *manual testing* dan *wordlist-based testing*. *Manual testing* menawarkan akurasi yang tinggi meski memerlukan waktu yang lebih lama, sedangkan *wordlist-based testing* adalah metode yang lebih cepat dan efisien, namun cenderung kurang fleksibel dalam mendeteksi variasi *payload* yang tidak ada dalam daftar.

6) Metode dan Teknik Pencarian *Open Redirect Payload*

Pencarian *Open Redirect Payload* juga melibatkan dua pendekatan utama: *manual testing* dan *wordlist-based testing*. *Manual testing* memberikan hasil yang sangat akurat namun memakan waktu, sementara *wordlist-based testing* lebih efisien dalam pengujian tetapi mungkin tidak selalu mencakup semua variasi *payload* yang potensial.

7) GH3RTZ *Framework* dalam Penerapan Tahap *Reconnaissance*

GH3RTZ *framework* mendukung tahap *reconnaissance* dengan menyediakan berbagai alat yang terintegrasi, seperti *Sublist3r* untuk enumerasi *subdomain* dan fitur untuk injeksi *XSS* serta *Open Redirect*. *Framework* ini dirancang untuk meningkatkan efisiensi dan kemudahan penggunaan dalam proses pengumpulan informasi awal, sehingga mempermudah penguji dalam identifikasi potensi kerentanan.

8) GH3RTZ *Framework* dalam Penerapan Tahap Pendeteksi Celah Keamanan

Dalam tahap pendeteksian celah keamanan, GH3RTZ *framework* efektif untuk mengidentifikasi kerentanan seperti *XSS* dan *Open Redirect*. Dengan fitur yang memungkinkan pengujian menyeluruh dan deteksi kerentanan dengan cepat, *framework* ini membantu penguji dalam menemukan dan mengatasi masalah keamanan dengan lebih efektif.

9) Evaluasi GH3RTZ *Framework* dalam Mendukung Tahap *Reconnaissance* dan Pendeteksi Celah Keamanan

Evaluasi GH3RTZ *framework* mencakup pengujian fungsionalitas, analisis performa, dan evaluasi keamanan. Proses ini bertujuan untuk menilai sejauh mana *framework* ini mendukung tahap *reconnaissance* dan pendeteksian celah keamanan, memastikan bahwa alat-alat yang disediakan efektif dan dapat diandalkan dalam pengujian keamanan.

10) Python

Python adalah bahasa pemrograman tingkat tinggi yang menekankan keterbacaan kode dan efisiensi penulisan dengan sintaks sederhana [5]. *Python* mendukung berbagai paradigma pemrograman seperti *OOP*, imperatif, dan fungsional. Dalam pengembangan web, *Python* menawarkan *framework* seperti *Django* dan *Flask*. *Django*, dengan prinsip "*batteries-included*", memudahkan pengembangan aplikasi web besar dengan fitur seperti *ORM* dan sistem autentikasi. Sebaliknya, *Flask* adalah *micro-framework* yang memberikan fleksibilitas lebih untuk aplikasi *web* yang sederhana dan disesuaikan. *Python* juga memiliki banyak pustaka dan komunitas yang besar, menjadikannya pilihan populer untuk pengembangan dan pengujian keamanan.

11) *Sublist3r*

Sublist3r adalah alat sumber terbuka untuk pencarian *subdomain* yang membantu dalam pengujian penetrasi dengan menggunakan mesin pencari dan layanan seperti *VirusTotal* [6]. Alat ini mengidentifikasi *subdomain* tersembunyi yang dapat menjadi titik lemah untuk serangan. *Sublist3r* memiliki antarmuka yang sederhana dan mendukung integrasi dengan alat lain, mempermudah otomasi dalam pengujian penetrasi. Integrasinya dengan OSINT juga memperkaya data yang dikumpulkan, menjadikannya alat yang berguna untuk analisis mendalam.

12) *Web Archives*

Arsip *web* menyimpan konten *web* historis dan sangat berharga untuk analisis keamanan siber. Alat seperti *Wayback Machine* memungkinkan peneliti untuk memeriksa evolusi kerentanan dan strategi keamanan dari waktu ke waktu [7]. Arsip ini membantu dalam memahami pola serangan dan efektivitas praktik keamanan, serta mendukung penelitian humaniora digital yang berkaitan dengan pelestarian konten web. Integrasi dengan alat digital lainnya meningkatkan kegunaan arsip *web* dalam analisis keamanan dan tata kelola *web* [8].

B. Data Penilitian

Data yang digunakan dalam penelitian ini meliputi website-website yang memiliki potensi kerentanan keamanan tinggi. Dua situs yang digunakan sebagai studi kasus adalah *http://zero.webappsecurity.com* dan *Damn Vulnerable Web Application (DVWA).* Kedua situs ini dipilih karena sering digunakan dalam pengujian keamanan *web* dan menyediakan berbagai skenario serangan yang relevan dengan tujuan penelitian ini.

Data yang digunakan mencakup:

1) *Wordlist* berisikan *payload* untuk *pencarian Cross Site Scripting (XSS).*

TABEL I
PAYLOAD XSS

Payload
'"><A HRef=\" AutoFocus OnFocus=top/**/?.['ale'%2B'rt'](1)>
<svg/onload=window["al"+"ert"]1337>
<Img Src=OnXSS OnError=confirm(1337)>
<Svg Only=1 OnLoad=confirm(document.domain)>
><script%20>alert(document.domain)<%2fscript>
<Img Src=OnXSS OnError=confirm("Hacked_by_mijan")>
<Img Src=//X55.is OnLoad%0C=import(Src)>
">'><details/open/ontoggle=confirm('XSS')>
<scr<script>ipt>alert('XSS+by+Givari+Ramadan') </scr<script>ipt><Svg Only=1 OnLoad=confirm(atob("Q2xvdWRmbGFyZSBCeXBhc3NlZCA6KQ=="))>

2) *Wordlist* berisikan *payload* untuk pencarian *Open Redirect*.

TABEL II
PAYLOAD OPEN REDIRECT

Payload
/%09/example.com
/%2f%2fexample.com
///example.com/
//google.com/%2f..
////example.com//
//google.com/
https:///www.google.com/%2e%2e
//https://www.whitelisteddomain.tld@www.google.com/%2e%2e%2f
///google.com//
https://google.com/

C. Penerapan Metode

Metode yang digunakan dalam penelitian ini adalah penerapan framework gh3rtz, yang berfokus pada tahap *reconnaissance* dan deteksi kerentanan keamanan pada situs web. *Framework* ini dirancang untuk mengotomatiskan proses pencarian *subdomain*, *parameter*, serta injeksi *XSS* dan *Open Redirect*. Berikut adalah tahapan penerapan metode yang digunakan:

1) Pengumpulan Dataset dan Identifikasi Target.
2) Pengembangan dan Pelatihan *Framework* gh3rtz.
3) Pengujian pada Situs Target.
4) Analisis dan Validasi Hasil Pengujian.
5) Penyusunan Laporan dan Hasil Akhir.

Tahap awal dalam penelitian ini melibatkan pengumpulan data dari situs target, yaitu *http://zero.webappsecurity.com* dan *Damn Vulnerable Web Application* (*DVWA*). Data yang dikumpulkan mencakup *subdomain, parameter* yang tersedia di halaman web, serta kemungkinan titik injeksi untuk serangan *XSS* dan *Open Redirect*. Dataset ini digunakan untuk menguji efektivitas *framework* gh3rtz dalam mendeteksi potensi kerentanan pada situs-situs tersebut.

Pada penelitian sebelumnya, metode manual testing sering digunakan dalam deteksi kerentanan, seperti yang dijelaskan dalam "Automation in Manual Penetration Testing

Using Bash Shell Script" oleh Aman Kumar Singh et al[9]. Metode manual ini memerlukan waktu dan tenaga yang signifikan karena penguji harus secara manual memeriksa setiap kemungkinan kerentanan, yang seringkali memerlukan keahlian khusus. Namun, penelitian ini tidak memberikan hasil yang konsisten karena ketergantungan pada faktor manusia, yang dapat mengakibatkan kelalaian dalam mendeteksi beberapa kerentanan. GH3RTZ framework dipilih sebagai solusi karena kemampuannya untuk mengotomatisasi proses ini, sehingga mengurangi kesalahan manusia dan mempercepat proses deteksi kerentanan.

Tahap kedua adalah pengembangan dan pelatihan *framework* gh3rtz. Proses ini melibatkan pemrograman fitur-fitur kunci dalam *framework*, seperti *Subdomain Finder*, *Parameter Finder*, *XSS Injection*, dan *Open Redirect Injection*. Masing-masing fitur ini dirancang untuk mengidentifikasi dan mengeksploitasi titik lemah dalam struktur situs *web*. Setelah pengembangan, *framework* diuji untuk memastikan fungsionalitasnya berjalan dengan baik dan dapat mendeteksi kerentanan dengan akurasi tinggi.

Pengujian pada Situs Target menggunakan *Grey Box Testing*. Tahap ini melibatkan penerapan *framework* gh3rtz pada situs target dengan pendekatan *Grey Box Testing*. Dalam jenis pengujian ini, peneliti bertindak sebagai *Penetration Tester* yang memiliki akses terbatas ke struktur internal situs *web* yang diuji, menyerupai skenario serangan oleh pengguna eksternal dengan pengetahuan parsial mengenai sistem. Pendekatan ini memberikan keuntungan karena tidak memerlukan akses ke kode sumber situs yang diuji, sekaligus meminimalkan potensi konflik antara pengembang dan tester[10]. Dalam proses ini, setiap fitur dari *framework* gh3rtz digunakan untuk menjalankan pengujian pada situs *web* yang telah dipilih. Misalnya, *Subdomain Finder* digunakan untuk menemukan *subdomain* tersembunyi, sementara *XSS Injection* dan *Open Redirect Injection* diujikan untuk mengeksploitasi titik-titik yang rentan terhadap serangan tersebut. Proses ini dirancang untuk mengidentifikasi kerentanan secara otomatis dan cepat.

Tahap selanjutnya adalah analisis dan validasi hasil pengujian. Setelah kerentanan terdeteksi, analisis dilakukan untuk menilai sejauh mana *framework* gh3rtz mampu mengidentifikasi celah keamanan yang relevan. Selain itu, hasil dari *framework* ini dibandingkan dengan hasil dari *framework* lain seperti *OWASP ZAP* dan Burp Suite untuk mengevaluasi keunggulan dan kelemahan gh3rtz. Validasi hasil dilakukan dengan mengonfirmasi keberadaan kerentanan yang telah ditemukan.

Tahap akhir dari penerapan metode ini adalah penyusunan laporan hasil penelitian. Laporan ini mencakup data yang telah dianalisis, perbandingan hasil pengujian dengan *framework* lain, dan kesimpulan mengenai efektivitas *framework* gh3rtz. Laporan ini juga memberikan rekomendasi untuk pengembangan lebih lanjut dari *framework* dan penggunaannya dalam praktik pengujian keamanan *web*.

III. HASIL DAN PEMBAHASAN

A. Pengujian Program

1) Analisis Hasil

Pengujian program ini melibatkan analisis hasil dari berbagai teknik pengujian seperti *subdomain enumeration*, parameter *crawling*, XSS *injection*, dan *open redirect injection*. Hasil dari setiap teknik ini dievaluasi untuk mengidentifikasi keberhasilan atau kegagalan dalam menemukan celah keamanan. Detail dari celah yang teridentifikasi dijelaskan secara rinci, termasuk proses injeksi yang dilakukan dan hasil yang diperoleh. Informasi ini krusial untuk memahami jenis-jenis kerentanan spesifik dan potensi eksploitasi oleh pihak yang tidak bertanggung jawab.

TABEL III
ANALISIS SUBDOMAIN FINDER

Domain	Hasil
Webappsecurity.com	Zero.webappsecurity.com
DVWA	Tidak Ditemukan

TABEL IV
ANALISIS HASIL PARAMETER FINDER

Domain	Hasil
http://zero.webappsecurity.com	http://zero.webappsecurity.com/search.html?searchTerm=FUZZ, http://zero.webappsecurity.com/banklogin.asp?templateName=FUZZ, http://zero.webappsecurity.com:80/help.html?topic=FUZZ, http://zero.webappsecurity.com/banklogin.asp?templateName=FUZZ&AD_REFERRING_URL=FUZZ
DVWA	http://localhost/DVWA/vulnerabilities/open_redirect/source/low.php?redirect=FUZZ, http://localhost/DVWA/vulnerabilities/open_redirect/source/medium.php?redirect=FUZZ

TABEL V
ANALISIS HASIL XSS INJECTION

Domain & Payload	Hasil
http://zero.webappsecurity.com/search.html?searchTerm <scr<script>ipt>alert('XSS+by+Givari+Ramadan') </scr<script>ipt>	*Suspicious (Potential False Positive)*

2) Hasil Injeksi Berhasil

Gambar 2 menunjukan jika injeksi berhasil, outputnya akan ditandai dengan warna merah. Ini menunjukkan bahwa serangan skrip berbahaya telah berhasil dieksekusi pada subdomain atau parameter tertentu. Contoh dari hasil ini dapat berupa tangkapan layar dari skrip yang dieksekusi atau pesan yang muncul di halaman *web* yang menunjukkan kerentanan. Informasi ini membantu dalam mengidentifikasi titik-titik yang memerlukan perbaikan segera untuk meningkatkan keamanan sistem.

TABEL VI
HASIL INJEKSI BERHASIL

Subdomain	*Parameter*	*Payload*	Hasil
DVWA	*Open_redirect/source/low.php?redirect=*	*http://evil.com*	Berhasil menuju ke halaman *evil.com*

Gambar 2. Hasil Injeksi Behasil

3) Hasil Injeksi Tidak Berhasil

Jika injeksi tidak berhasil, pada tabel 7 ditunjukkan outputnya akan ditampilkan dalam warna hijau. Hal ini menunjukkan bahwa upaya untuk mengeksploitasi celah keamanan tidak berhasil. Penjelasan kemungkinan alasan kegagalan serta langkah-langkah yang bisa diambil untuk memperbaiki situasi ini juga akan disediakan. Misalnya, dalam kasus pengujian *Open Redirect Injection*, ini bisa menunjukkan bahwa subdomain mungkin sudah dilindungi dengan baik melalui validasi URL yang ketat.

TABEL VII
HASIL INJEKSI TIDAK BERHASIL

Subdomain	*Parameter*	*Payload*	Hasil
DVWA	*Open_redirect/source/ medium.php?redirect=*	*http://evil.com*	Tidak berhasil menuju ke halaman *evil.com*

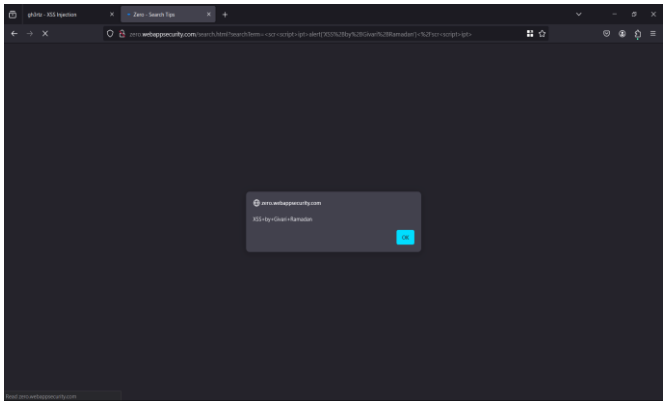
4) Hasil Injeksi Tidak Berhasil

Gambar 3 menunjukan hasil dinyatakan false positive, yang ditandai dengan warna kuning, menunjukkan bahwa meskipun ada indikasi potensial celah keamanan, perlu dilakukan pemeriksaan lebih lanjut secara manual untuk memverifikasi keberadaan celah tersebut. Ini bisa terjadi ketika alat atau metode pengujian otomatis menghasilkan kesalahan dalam mengidentifikasi kerentanan yang sebenarnya tidak ada. Dalam hal ini, penting untuk melakukan peninjauan manual lebih lanjut untuk mengonfirmasi keberadaan atau ketiadaan kerentanan sebelum mengambil tindakan lebih lanjut.

TABEL VIII
HASIL INJEKSI FALSE POSITIVE

Subdomain	*Parameter*	*Payload*	Hasil
Zero.webapps ecurity.com	*search.html ?searchTer m=*	*<scr<script>ipt>al ert('XSS+by+Givari +Ramadan')</scr<s cript>ipt>*	False Positive tetapi berhasil mengeksekusi payload

Gambar 3. Hasil Injeksi *False Positive*



Gambar 4. *Payload* Berhasil Ter-Eksekusi

Hasil ini memberikan gambaran menyeluruh tentang hasil pengujian program, termasuk analisis mendalam dari setiap teknik yang digunakan dan implikasi keamanan yang relevan. Informasi ini tidak hanya membantu dalam memperbaiki kelemahan yang teridentifikasi, tetapi juga meningkatkan pemahaman tentang kompleksitas dalam melindungi aplikasi web dari berbagai ancaman keamanan.

IV. KESIMPULAN

Berdasarkan Berdasarkan penelitian mengenai "Pembuatan GH3RTZ *Framework* sebagai Penggunaan Proses Tahapan *Reconnaissance* dan Pendeteksi Celah Keamanan," dapat disimpulkan bahwa GH3RTZ *framework* terbukti mampu mendeteksi kerentanan keamanan pada tahap *reconnaissance*. *Framework* ini membantu pemilik situs web dalam mengambil langkah pencegahan awal yang sangat penting, sebuah aspek yang belum banyak diimplementasikan dalam *framework* sejenis. Dengan menggunakan Algoritma *Boyer-Moore*, GH3RTZ *framework* mampu meningkatkan pencarian dan identifikasi kerentanan keamanan, menjadikannya salah satu *framework* yang secara khusus mengintegrasikan algoritma ini untuk keamanan siber.

Selain itu, GH3RTZ *framework* tidak hanya berfungsi sebagai alat deteksi kerentanan, tetapi juga berperan dalam meningkatkan kesadaran keamanan di kalangan pemilik dan pengembang situs web melalui proses otomatisasi yang diimplementasikan dengan baik. *Framework* ini dirancang dengan kemudahan implementasi, yang membuatnya sangat berguna bagi usaha kecil dan menengah dengan sumber daya yang terbatas, sesuatu yang jarang ditemukan dalam *framework* sejenis.

Penelitian ini memberikan kontribusi unik dalam pengembangan alat deteksi kerentanan keamanan yang menggabungkan metode *reconnaissance* otomatis dengan algoritma pencarian yang baik, sehingga memperkaya bidang keamanan siber dan menawarkan pendekatan baru yang belum banyak dieksplorasi dalam penelitian sebelumnya. Ke depannya, diharapkan GH3RTZ *framework* dapat menjadi alat yang bermanfaat bagi pemilik dan pengembang situs web dalam meningkatkan keamanan digital mereka.

Sebagai saran untuk penelitian selanjutnya, disarankan untuk mengembangkan *framework* ini agar lebih adaptif terhadap berbagai jenis serangan yang terus berkembang di

dunia siber. Penelitian lebih lanjut juga dapat difokuskan pada peningkatan kemampuan *framework* untuk mendeteksi kerentanan di lingkungan yang lebih kompleks, serta menguji efektivitasnya dalam skenario serangan nyata. Dengan begitu, *framework* ini dapat terus ditingkatkan dan disesuaikan dengan kebutuhan keamanan yang dinamis.

REFERENSI

[1] A. Rayhan, "Cybersecurity in the Digital Age: Assessing Threats and Strengthening Defenses," *Conference: Cybersecurity Awareness*, April, 2024, pp. 1-26.

[2] D. Ghelani, "Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review," *American Journal of Science, Engineering and Technology*, vol. 3, no. 6, pp. 12–19, 2022.

[3] K. Abdulghaffar, N. Elmrabit, and M. Yousefi, "Enhancing Web Application Security through Automated Penetration Testing with Multiple Vulnerability Scanners," *Computers*, vol. 12, no. 11, pp. 1-17, 2023.

[4] Y. Faqih, Y. Rahmanto, A. Ari Aldino, and B. Waluyo, "Penerapan String Matching Menggunakan Algoritma Boyer-Moore Pada Pengembangan Sistem Pencarian Buku Online," *Bulletin of Computer Science Research*, vol. 2, no. 3, pp. 100–106, 2022.

[5] A. Rawat, "A Review on Python Programming," *International Journal of Research in Engineering, Science and Management*, 2020.

[6] I. Böhm and S. Lolagar, "Open source intelligence," *International Cybersecurity Law Review*, vol. 2, no. 2, pp. 317–337, 2021.

[7] K. Teszelszky, "Introduction: digital humanities and the use of web archives," *International Journal of Digital Humanities*, vol. 2, no. 1–3, pp. 1–4, 2021.

[8] V. Schafer and J. Winters, "The values of web archives," *International Journal of Digital Humanities*, vol. 2, no. 1–3, pp. 129–144, Nov. 2021.

[9] A. K. Singh, G. Kumar, and K. Vishwakarma, "Automation In Manual Penetration Testing Using Bash Shell Script," International Research Journal of Modernization in Engineering Technology and Science, May 2023.

[10] P. Vats, M. Mandot, and A. Gosain, "A Comprehensive Literature Review of Penetration Testing Its Applications," in ICRITO 2020 - IEEE 8th International Conference on Reliability, *Infocom Technologies and Optimization (Trends and Future Directions)*, Institute of Electrical and Electronics Engineers Inc., Jun. 2020, pp. 674–680.